**Computer Security**

https://encyclopedia2.thefreedictionary.com/Cyber+security

The process of ensuring confidentiality, integrity, and availability of computers, their programs, hardware devices, and data. Lack of security results from a failure of one of these three properties. The lack of confidentiality is unauthorized disclosure of data or unauthorized access to a computing system or a program. A failure of integrity results from unauthorized modification of data or damage to a computing system or program. A lack of availability of computing resources results in what is called denial of service.

An act or event that has the potential to cause a failure of computer security is called a threat. Some threats are effectively deflected by countermeasures called controls. Kinds of controls are physical, administrative, logical, cryptographic, legal, and ethical. Threats that are not countered by controls are called vulnerabilities.

**Encryption**

Encryption is a very effective technique for preserving the secrecy of computer data, and in some cases it can also be employed to ensure integrity and availability. An encrypted message is converted to a form presumed unrecognizable to unauthorized individuals. The principal advantage of encryption is that it renders interception useless.

**Access control**

Computer security implies that access be limited to authorized users. Therefore, techniques are required to control access and to securely identify users. Access controls are typically logical controls designed into the hardware and software of a computing system. Identification is accomplished both under program control and by using physical controls.

Typically, access within a computing system is limited by an access control matrix administered by the operating system or a processing program. All users are represented as subjects by programs executing on behalf of the users; the resources, called the objects of a computing system, consist of files, programs, devices, and other items to which users' accesses are to be controlled. The control matrix specifies for each subject the objects that can be accessed and the kinds of access that are allowed.

Access control as described above relates to individual permissions. Typically, such access is called discretionary access control because the control is applied at the discretion of the object's owner or someone else with permission. With a second type of access control, called mandatory access control, each object in the system is assigned a sensitivity level, which is a rating of how serious would be the consequences if the object were lost, modified, or disclosed, and each subject is assigned a level of trust.

Access control is not necessarily as direct as just described. Unauthorized access can occur through a covert channel. One process can signal something to another by opening and closing files, creating records, causing a device to be busy, or changing the size of an object. All of these are acceptable actions, and so their use for covert communication is essentially impossible to detect, let alone prevent.

**Security of programs**

Computer programs are the first line of defense in computer security, since programs provide logical controls. Programs, however, are subject to error, which can affect computer security.

A computer program is correct if it meets the requirements for which it was designed. A program is complete if it meets all requirements. Finally, a program is exact if it performs only those operations specified by requirements.

Simple programmer errors are the cause of most program failures. Fortunately, the quality of software produced under rigorous design and production standards is likely to be quite high. However, a programmer who intends to create a faulty program can do so, in spite of development controls**.**

A salami attack is a method in which an accounting program reduces some accounts by a small amount, while increasing one other account by the sum of the amounts subtracted. The amount reduced is expected to be insignificant; yet, the net amount summed over all accounts is much larger.

Some programs have intentional trapdoors, additional undocumented entry points. If these trapdoors remain in operational systems, they can be used illicitly by the programmer or discovered accidentally by others.

A Trojan horse is an intentional program error by which a program performs some function in addition to its advertised use. For example, a program that ostensibly produces a formatted listing of stored files may write copies of those files on a second device to which a malicious programmer has access.

A program virus is a particular type of Trojan horse that is self-replicating. In addition to performing some illicit act, the program creates a copy of itself which it then embeds in other, innocent programs. Each time the innocent program is run, the attached virus code is activated as well; the virus can then replicate and spread itself to other, uninfected programs. Trojan horses and viruses can cause serious harm to computing resources, and there is no known feasible countermeasure to halt or even detect their presence.

**How Trojan Horses Work**

One of the most enduring stories of the Trojan War, the most important conflict in Greek mythology, is the tale of the Trojan horse. Trying to find a way into the city of Troy, the great warrior Odysseus ordered his men to build a massive wooden horse, one big enough for several Greek soldiers to fit in. Once the structure was finished, he and several other warriors climbed inside, while the rest of the Greeks sailed away from Troy. One man named Sinon, however, stayed behind in order to deceive the Trojans, convincing them that his fellow Greeks had betrayed him and fled from the city. The wooden horse, he told the Trojans, was safe and would bring them luck.

After some discussion over the matter, the Trojans agreed to wheel the horse through their gates, unknowingly giving the Greek enemy access to the city. After proclaiming victory and partying all night, the citizens of Troy went to sleep – it was then that Odysseus and his men crept out of the Trojan horse and wreaked havoc on the city.

Although you've probably heard of the Trojan horse from Greek mythology, chances are you've also heard of Trojan horses in reference to computers. Trojan horses are common but dangerous programs that hide within other seemingly harmless programs. They work the same way the ancient Trojan horse did: Once they're installed, the program will infect other files throughout your system and potentially wreak havoc on your computer. They can even send important information from your computer over the Internet to the developer of the virus. The developer can then essentially control your computer, slowing your system's activity or causing your machine to crash.

Though they're not actually viruses, they're referred to as "Trojan horse viruses," "Trojan viruses," "Trojan horses" or just plain "Trojans." Regardless of what people call them, they all mean the same thing. But what happened? How did you let this Trojan horse into your computer in the first place? And what can you do to stop one from getting in?

**Protecting Yourself from Trojan Horses**

So how do Trojan horses infect computers? Believe it or not, you have to do some of the work yourself. In order for a Trojan to infect your machine, you have to install the server side of the application. This is normally done by social engineering – the author of the Trojan horse has to convince you to download the application. Alternately, he or she might send the program to you in an e-mail message hoping you execute it. Again, this is why it is called a Trojan horse – you have to consciously or unconsciously run the .exe file to install the program – it doesn't propagate on its own like a virus. Once you execute the program, the Trojan server is installed and will start running automatically every time you power up your computer.

The most common way Trojan horses spread is through e-mail attachments. The developers of these applications typically use spamming techniques to send out hundreds or even thousands of e-mails to unsuspecting people; those who open the messages and download the attachment end up having their systems infected.

Sometimes, it's not even a person manually spreading malware -- it's possible for your own computer to do so, if it's been infected already. Crackers – hackers who use their computer skills to create mischief or cause damage intentionally – can send out Trojans that turn innocent Web surfer's computers into zombie computers, so-called because the person with the infected computer rarely knows his system is under control. Crackers then use these zombie computers to send out more viruses, eventually creating networks of zombie computers known as botnets.

There are several things you can do to protect yourself from Trojan horses. The easiest thing to do is to never open any e-mails or download any attachments from unknown senders. Simply deleting these messages will take care of the situation. Installing antivirus software will also scan every file you download (even if it's from someone you know) and protect you from anything malicious. If you ever find your computer has been infected with a Trojan, you should disconnect your Internet connection and remove the files in question with an antivirus program or by reinstalling your operating system. You can call your computer's manufacturer, your local computer store or a knowledgeable friend if you need help.